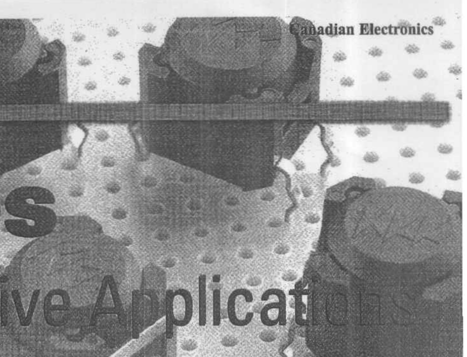


Windowed Watchdog Increases Fault Coverage in Sensitive Applications

By Donald W. Corson

All developers of embedded microprocessor systems know standard watchdog timers. They form part of the first line defense against malfunctioning processors, be it because of system instability, external disturbances or through real-life situations bringing the system in untested states. These watchdog circuits are ubiquitous either as standalone chips or internal to the microcontrollers themselves. In systems where human safety is involved, even higher standards of reliability are required.

For these cases the external windowed watchdog timer is indicated. These applications include automotive applications like anti-lock brakes and steering systems, medical instruments like insulin pumps, robots, industrial control and automatic doors, nuclear power plant controls and avionics. These systems must be able to recover from a crash without human assistance, pressing a reset button for example, as any human intervention would probably be too late to avoid injury.

While microprocessors are highly flexible problem solution tools, their functional reliability is lowered by the probability of code errors in the program. Defensive programming techniques such filling unused ROM with HALT or illegal instructions to trap illegal jumps in code space will aid in program debugging. They can also give a small handle for gracious recovery when deployed, but even with the most careful and complete testing not all errors will be found, 100% coverage can never be assured.

Ideally, a watchdog-monitored system is able to restart itself back into a working state and the user will not even know that an error has occurred. To achieve this level of comfort, the system must be conceived and the software programmed to be able to accept a reset at any time and to resume normal operation without any operator intervention.

Many microcontrollers offer an internal programmable watchdog with similar functionality. These watchdogs can, however, all be disabled by the software and do not provide the same protection for safety critical applications as an independent external watchdog timer circuit. Therefore, it is highly recommended to use an external watchdog and reset circuit in critical applications.

Operation of Windowed Watchdog Timers

Standard watchdog timers (WDT) are incrementing counters that set their output if their maximum value is reached. The microcontroller must reset the counter before that happens by creating an edge on the timer clear input. If the program execution is faulty because of a program error or external disturbance causing the program execution to be slower, the maximum value will be reached and the output set active. This will catch problems such as hanging because of endless loops. It will not, however, trigger for such errors as routines returning before normal completion, which will cause the program execution to be faster.

For highest security, a windowed watchdog timer (WWDT) demands that the timer clear input edge be within a certain timing window that is considered correct. If the signal arrives before or after this timing window it triggers the output signal to either reset the processor or activate other error handling. This type of watchdog will effectively cover both the case of a program executing too slowly and the case of a program executing to quickly. Another observed cause of error is crystals jumping to spurious modes because of external shocks. Although in this case the crystal will probably return to its proper frequency after a short time, the processor may be in danger of improper program execution during this time. The windowed watchdog can catch this behavior.

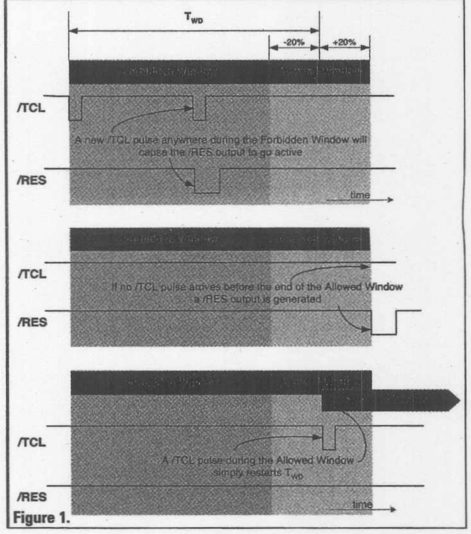

T_WD
-20%
+20%
/TCL
A new /TCL pulse anywhere during the Forbidden Window will cause the /RES output to go active
/RES
time
/TCL
If no /TCL pulse arrives before the end of the Allowed Window a /RES output is generated
/RES
/TCL
A /TCL pulse during the Allowed Window simply restarts T_WD
/RES
time

Figure 1.

To understand the real difference of thinking between a standard WDT and a WWDT, consider of the following: a standard watchdog timer assumes that everything is OK in the system unless it receives no signal from the system. A WWDT on the other hand assumes that there is a problem in the system, unless it receives a signal at the right time. Viewed this way, it is easy to see how the WWDT increases the coverage of system errors recognized.

The watchdog timing is broken into two periods. The time when the /TCL falling flank signals an error is called the 'forbidden window'. The time when the /TCL input falling flank resets the timer, is accepted, is called the 'allowed window'. In some documentation the allowed window is called the 'open window' and the forbidden window is called the 'closed window'. After the allowed window the windowed watchdog times out causing the tor and the Allowed Window is during the time + 20% of the watchdog time T_{WD}. The Forbidden Window is during the time up to 80% of T_{WD}. The watchdog timeout is at T_{WD} + 20%. Please see Figure 1. If no /TCL has been received until the end of the allowed window the watchdog will immediately produce a reset pulse. Both a falling flank on /TCL during the forbidden window and a timeout after T_{WD}+20% will cause a reset to be asserted and the enable to be removed. It should be noted that the timing for the next period starts immediately from the falling flank of /TCL.

The Important Difference

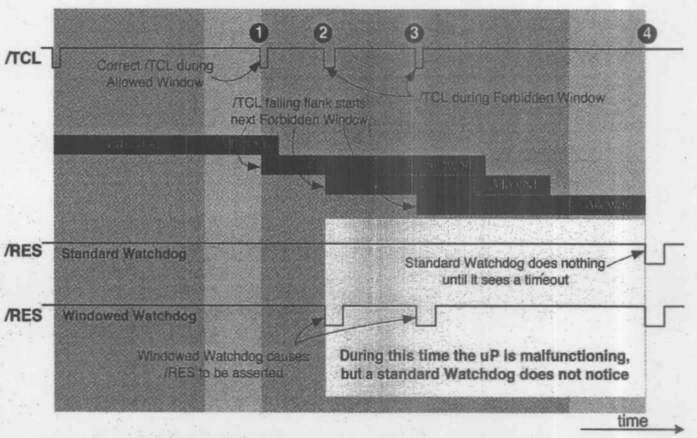
To understand the benefits of using a WWDT over a standard WDT for high reliability applications refer to Figure 2.

In this diagram we can see the following: At (1) a correct /TCL input during the allowed window. At (2) and (3) the /TCL signal is shown arriving too early, during the forbidden window. This results in the /RES output being asserted immediately by the windowed watchdog timer. A standard watchdog would not notice this malfunction. It is just at (4) where no /TCL signal arrives before the end of the watchdog timeout that a standard watchdog would react by asserting /RES, as does the windowed watchdog too. It can be seen that in each case the watchdog timing is counted from the falling flank of the last /TCL input.

Many WWDT chips also offer an increased confidence enable output /EN. The increased confidence enable output /EN can be used to gate motor signals, for instance, to immediately stop the motor movement when the processor behavior can not be trusted and only allow it again when there is confidence that the processor is running properly. This signal is only asserted after three good /TCL flanks have been seen and is removed simultaneously with the /RES output assertion in case of a detected malfunction of the processor.

WWDT circuits generally also include all the features of a standard voltage supervisory circuit and are available in versions with and without an accurate protected 5V low-dropout voltage regulator. These circuits are particularly indicated for decentralized systems such as in automotive and industrial automation applications as they can monitor the security and provide the power supply regulation in one component.

Distributed systems in general are another application where windowed watchdogs are a powerful help in maintaining confidence in the total system. In systems where a master provides timing or synchronization messages to the slave processors a standard watchdog can detect a missing or failing slow master. A windowed watchdog increases the error coverage to failing fast or multiple conflicting masters on the bus


1
2
3
4
/TCL
Correct /TCL during Allowed Window
/TCL falling flank starts next Forbidden Window
/TCL during Forbidden Window
/RES
Standard Watchdog
Standard Watchdog does nothing until it sees a timeout
/RES
Windowed Watchdog
Windowed Watchdog causes /RES to be asserted
During this time the uP is malfunctioning, but a standard Watchdog does not notice
time

A Windowed Watchdog Timer provides complete error coverage in all situations

Figure 2.

Application example

Windowed Watchdog

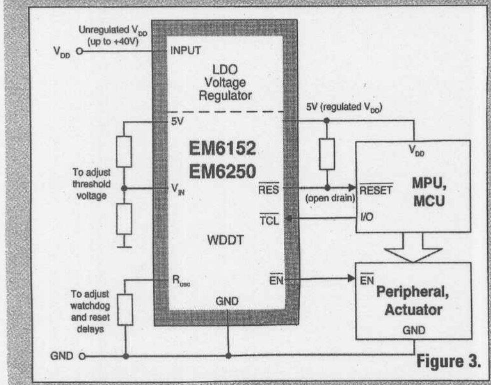


Figure 3.

(Continued from page 10)

success of the design. The routing of the decoupling capacitors to the supply and ground traces or planes must be clean and short. Circuitous paths increase the circuit inductance and possibly increase the cross coupling between inputs and outputs. Clean separation between logic supply and the power portion of the circuitry is especially important in circuits controlling electrical motors with the large spikes that they will produce on the power supply lines.

Conclusion

Including an internal voltage regulator and complete power supply supervision, a windowed watchdog such as the EM Microelectronics EM6250 and EM6152, provides greatly improved error case coverage compared to a standard watchdog and lends itself admirably for applications requiring stringent security surveillance in today's distributed intelligence automotive and industrial systems.

Just a short list of automotive application areas could include:

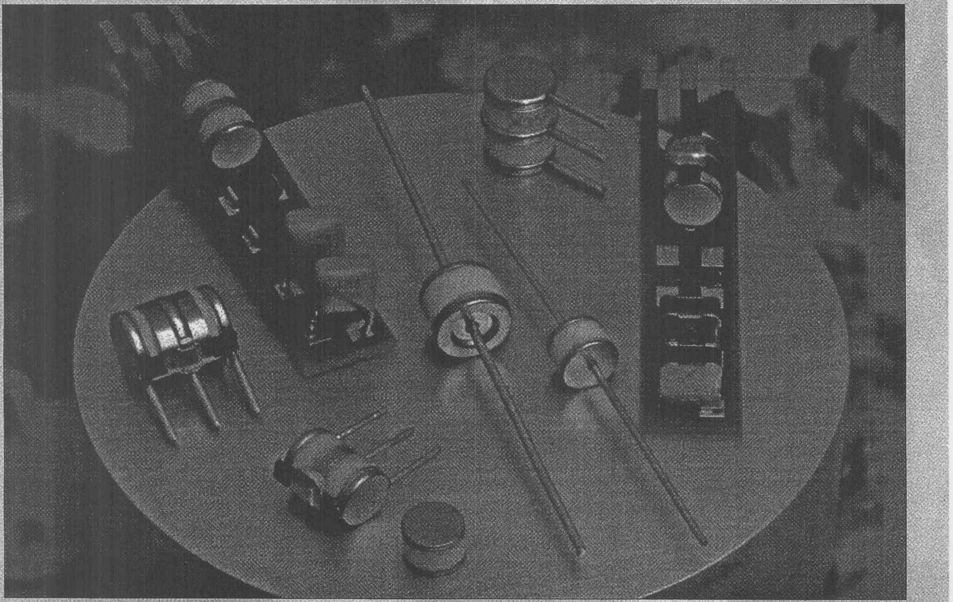
- window motor control
- sunroof motor control
- dashboard computer systems
- angular steering sensors
- trunk closure systems
- cruise control
- spoiler automatic
- automatic sliding door control
- automatic transmission control
- motor control

Watchdog components that can recognize being placed in sleep mode and adapt their behavior to reduce system power consumption without loosing security are also available on the market. These are ideal for ultra-low power applications using sleep mode, such as those using CAN-Bus communication, where functional units can be disabled under software control.

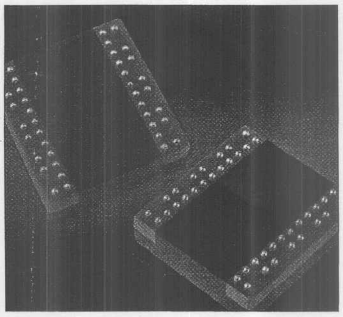
For safety critical applications such as medicine delivery devices, medical monitoring systems, robots and automatic doors and windows, wherever they may be installed, a windowed watchdog timer is the component of choice to be sure to fulfill the demands of regulating bodies in terms of human safety.

Donald W. Corson is with EM Microelectronic-Marin.

Circle CE 331



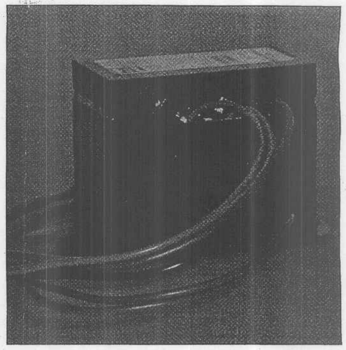
Circuit Protection & Switches



PLANAR BGA REED RELAY

Coto Technology has introduced the B41, a four independent channel, form-A, planar BGA reed relay. No slot or hole in the PC board is required to mount the device — a feature which simplifies the design of multi-layer boards. Coto's technology also allows for shorter RF paths in a controlled 50 ohm environment to minimize signal attenuation. Each channel has an RF insertion loss (-3dB roll-off point) of >8 GHz.

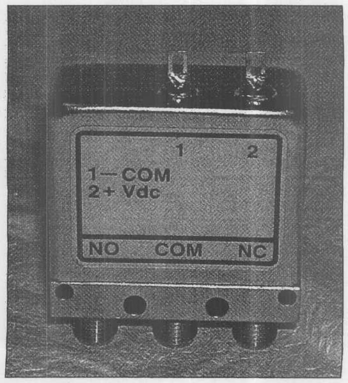
cotorelay.com **Circle CE 315**



TRANSFORMERS WITHSTAND SHORT CIRCUIT

Foster Transformer introduces the Survivor Class 2 transformer with short circuit and overload protection capable of withstanding a direct short circuit in excess of 15 days. All Survivor transformers including the 75 VA and 100 VA models are classified as inherently limited. This eliminates the need for external protection or the problematic internal fusing. It also extends the range of class 2 transformers allowing them to be used in intermittent duty applications that would cause the some fuses or circuit breakers to open.

foster-transformer.com **Circle CE 329**



18GHz RF SWITCH BOOSTS FREQUENCY

The 50S-1313 is a P2T, failsafe RF switch from JFW Industries. It boasts a frequency range of DC-18GHz with a maximum insertion loss of